COMPLETE LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claim 1 (previously presented): A cryptographic communication system comprising:

a plurality of user communication interfaces, each of said communication interfaces including:

a data transceiver;

a string generator;

a data processor connected to said string generator; and

a memory connected to said string generator, said memory having stored a unique seed value and a common seed value,

wherein the data processor processes data received by or to be transmitted by the data transceiver using data string generated by the string generator,

wherein the unique seed value for each of said plurality of user communication interfaces are unique to the respective communication interface, and wherein the common seed value stored in the memory of each of said plurality of communication interfaces is common to all of the plurality of communication interfaces, and

wherein the string generator generates data string using the unique seed value if the data to be transmitted or received by the data transceiver is unicast data intended to be received by one of said plurality of communication interfaces, and generates data string using the common seed value if the data received is designated as multicast data intended to be received by all of said plurality of communication interfaces; and

a master station, said master station including:

a data transceiver;

a second string generator;

a second data processor connected to said second string generator; and

a second memory connected to said second string generator, said second memory having stored each of the unique seed value stored in the plurality of communication interfaces and the common seed value,

wherein the second data processor processes data to be transmitted by or received by the data transceiver using data string generated by the second string generator, and

wherein the second string generator generates data string using one or more of the unique seed values if the data to be transmitted by or received by the data transceiver is intended to be received by select ones of said plurality of communication interfaces, and generates data string using the common seed value if the data to be transmitted is intended to be received by all of the plurality of communication interfaces.

Claim 2 (original): The cryptographic communication system according to claim 1,

wherein said string generator is a pseudo-random string generator, and

wherein said second string generator is a pseudo-random string generator.

Claim 3 (previously presented): The cryptographic communication system according to claim 1,

wherein each of said plurality of user communication interface further includes a key block formation device, and

wherein said master station further includes a second key block formation device.

Claim 4 (previously presented): The cryptographic communication according to claim 1, wherein each of said plurality of user communication interface is connected to said master station through a communication network.

Claim 5 (previously presented): The cryptographic communication according to claim 1, wherein each of said plurality of user communication interface communicates with the master station via a wireless network.

Claims 6-7 (canceled)

Claim 8 (previously presented): The cryptographic communication system according to claim 1,

wherein said second memory of said master station stores a user address value for each of said plurality of user communication interface.

Claim 9 (previously presented): The cryptographic communication system according to claim 8, wherein each of the unique seed values stored in said second memory is referenced to by the user address value corresponding to the user communication interface in which the unique seed value is stored.

Claim 10 (previously presented): The cryptographic communication system according to claim 1,

wherein said second memory of said master station stores a user identification for each of said plurality of user communication interface.

Claim 11 (previously presented): The cryptographic communication system according to claim 10, wherein each of the unique seed values stored in said second memory is referenced to by the user identification corresponding to the user communication interface in which the seed value is stored.

Claims 12-15 (canceled)

Claim 16 (currently amended): A method of cryptographic communication comprising the steps of:

storing in a memory a unique seed and a common seed;

generating a unique cryptographic key using the unique seed;

generating a common cryptographic key using the common seed;

receiving a signal;

detecting whether the signal is a unicast signal or a multicast signal;

selecting the unique cryptographic key if the signal received is detected to be a unicast signal;

selecting the common cryptographic key if the signal received is detected to be a multicast signal; and

applying the selected cryptographic key to the received signal

~~generating a data string using the unique seed if the signal is detected to be a unicast signal, and generating a data string using the common seed if the signal is detected to be a multicast signal;~~

~~forming an encryption key using the generated data string if the signal is to be transmitted, and encrypting the signal prior to transmitting the signal; and~~

~~forming a decryption key using the generated data string if the signal is not to be transmitted, and decrypting the received signal using said decryption key~~.

Claim 17 (currently amended): The method of cryptographic communication according to claim 16, wherein~~, when~~ a series of ~~data strings~~ unique and common cryptographic keys are periodically generated from ~~either~~ the unique seed ~~or from~~ and the common seed, respectively, wherein the series of ~~data strings are~~ unique and common cryptographic keys are generated in a pseudo-random order.

Claim 18 (original): The method of cryptographic communication according to claim 16, further comprising the step of determining whether the received signal is encrypted.

Claims 19-23 (canceled)

Claim 24 (original): The method of cryptographic communication according to claim 16, further comprising the step of transmitting a user address or a user identification.

Claims 25-37 (canceled)

Claim 38 (currently amended): A computer readable medium including executable instructions for causing a processor to perform a method of cryptographic communication, said method comprising the following steps:

storing in a memory a unique seed and a common seed;

generating a unique cryptographic key using the unique seed;

generating a common cryptographic key using the common seed;

receiving a signal;

detecting whether the signal is a unicast signal or a multicast signal;

selecting the unique cryptographic key if the signal received is detected to be a unicast signal;

selecting the common cryptographic key if the signal received is detected to be a multicast signal; and

applying the selected cryptographic key to the received signal

~~generating a data string using the unique seed if the signal is detected to be a unicast signal, and generating a data string using the common seed if the signal is detected to be a multicast signal;~~

~~forming an encryption key using the generated data string if the signal is to be transmitted, and encrypting the signal prior to transmitting the signal; and~~

~~forming a decryption key using the generated data string if the signal is not to be transmitted, and ; and decrypting the received signal using said decryption key~~.

Claim 39 (currently amended): The computer readable medium of claim 38, wherein~~, when~~ a series of ~~data strings~~ unique and common cryptographic keys are periodically generated from ~~either~~ the unique seed ~~or from~~ and the common seed, respectively, wherein the series of ~~data strings are~~ unique and common cryptographic keys are generated in a pseudo-random order.

Claim 40 (original): The computer readable medium of claim 38, wherein said method further comprises the step of determining whether the received signal is encrypted.

Claims 41-46 (canceled)

Claim 47 (original): The computer readable medium of claim 38, wherein said method further comprises the step of transmitting a user identification.

Claims 48-60 (canceled)

Claim 61 (currently amended): A method of cryptographic communication using a system having a plurality of user communication interfaces and a master station, wherein each of said plurality of user communication interfaces include a data transceiver, a string generator, a data processor connected to said string generator, and a memory connected to said string generator, said memory having stored a unique seed value, and wherein said master station includes a data transceiver, a string generator, a data processor connected to said string generator, and a memory connected to said string generator, said memory of the master station having stored the unique seed values of each of said plurality of user communication interfaces, wherein each of the unique seed

values stored at the memory of the master station are stored in correspondence to an identification of the corresponding user communication interface, said method comprising the steps of:

receiving an encrypted signal from one of the user communication interfaces, said encrypted signal addressed to be received by another one of the user communication interfaces, and said encrypted signal being encrypted using a cryptographic key generated by the string generator of said one user communication interface as a function of the unique seed value of said one user communication interface;

determining the identification of said one user communication interface sending the encrypted signal;

retrieving, from the memory of the master station, the unique seed value corresponding to the identified one user communication interface;

generating a cryptographic key using the unique seed value retrieved that corresponds to the identified one user communication interface;

decrypting said encrypted signal using said generated cryptographic key;

determining the identification of the other user communication interface;

retrieving, from the memory of the master station, the unique seed value corresponding to the other user communication interface;

generating a cryptographic key using the retrieved unique seed value corresponding to the other user communication interface;

re-encrypting the decrypted signal using the cryptographic key generated using the retrieved unique seed value corresponding to the other user communication interface; and

transmitting the re-encrypted signal to the other communication interface.